1. 網路流量及系統資源監控軟體(MRTG)安裝設定

## MRTG安裝設定說明

針對網路流量及與系統資源監控流量進行監控，以確保業者能即時發現網路攻擊行為。

* Linux環境
* ubuntu 14.04
* snmpd 5.7.2
* Apache 2.4.7
* MRTG 2.17.4
* Windows環境
* Windows 7專業版x64
* IIS7.5

## Linux系統安裝說明

#### 開啟終端機後，使用以下指令安裝apache, snmp, snmpd, 以及mrtg，若有已經安裝過的服務可略過該套件。

|  |
| --- |
| sudo apt-get install snmp snmpd apache2 mrtg |

#### 編輯/etc/snmp/snmpd.conf檔案。消除#號，反註解1；加上#號，註解2，詳見圖1。

|  |
| --- |
|  |
| 行政院國家資通安全會報技術服務中心整理 |
| 1. 編輯/etc/snmp/snmpd.conf檔案 |

#### 輸入以下指令重啟snmpd服務，並測試SNMPWALK是否正常運作。

|  |
| --- |
| sudo service snmpd restart  sudo snmpwalk localhost -c public -v 1 |

#### 創建MRTG所需設定檔並輸出。創建MRTG之index檔並輸出。若有參數與實際狀況不同，請自行修改。

|  |
| --- |
| sudo cfgmaker --output=/etc/mrtg.cfg public@127.0.0.1  sudo indexmaker --output=/var/www/html/mrtg/index.html /etc/mrtg.cfg |

#### 新增crontab，使MRTG自動每5分鐘進行更新。

|  |
| --- |
| crontab -e  \*/5 \* \* \* \* env LANG=C /usr/bin/mrtg /etc/mrtg.cfg |

#### 開啟/var/www/html/mrtg目錄中的網頁檔即可觀察視覺化的流量，詳見圖2。

|  |
| --- |
|  |
| 行政院國家資通安全會報技術服務中心整理 |
| 1. MRTG視覺化的流量 |

## Windows系統安裝說明

#### 點選開始功能表，搜尋開啟或關閉後，點擊開啟或關閉Windows功能，詳見圖3。

|  |
| --- |
|  |
| 行政院國家資通安全會報技術服務中心整理 |
| 1. 開啟或關閉Windows功能 |

#### 勾選簡易網路管理通訊協定(SNMP)與其子選項WMI SNMP提供者，詳見圖4。

|  |
| --- |
|  |
| 行政院國家資通安全會報技術服務中心整理 |
| 1. 啟用SNMP |

#### 點選開始功能表，搜尋「services.msc」後，點擊services，詳見圖5。

|  |
| --- |
|  |
| 行政院國家資通安全會報技術服務中心整理 |
| 1. 啟動services.msc |

#### 選取「SNMP Services」，雙擊後依圖片上之順序操作，詳見圖6。

|  |
| --- |
|  |
| 行政院國家資通安全會報技術服務中心整理 |
| 1. SNMP Services設定 |

#### 依系統類型至http://www.activestate.com/activeperl/downloads下載並安裝32位元或64位元主程式，詳見圖7。

|  |
| --- |
|  |
| 行政院國家資通安全會報技術服務中心整理 |
| 1. Perl程式下載 |

#### 至http://oss.oetiker.ch/mrtg/pub/?M=D下載最新.zip檔，並解壓縮在欲存放的資料夾目錄(以C:\為範例)。

#### 點選開始功能表，搜尋cmd後，點擊cmd。

#### 輸入以下指令以建立MRTG所需要的設定檔，詳見圖8。

|  |
| --- |
| cd C:\mrtg-2.17.4\bin  perl cfgmaker public@127.0.0.1 --global "WorkDir: C:\inetpub\wwwroot\mrtg" --output mrtg.cfg |

以下參數可依需求自行調整:

* 127.0.0.1：欲偵測的網卡IP或網域名稱
* WorkDir: 存放結果的目錄
* mrtg.cfg: 設定檔名稱

|  |
| --- |
|  |
| 行政院國家資通安全會報技術服務中心整理 |
| 1. 建立MRTG所需要的設定檔 |

#### 編輯bin資料夾中的mrtg.cfg，在檔案末端加入RunAsDaemon：yes。

#### 在Windows啟動資料夾中(預設C:\Users\fchiao\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup)新建MRTG.bat檔，輸入以下內容並存檔，每次重開機皆可自動啟動與監控流量，詳見圖9。

|  |
| --- |
|  |
| 行政院國家資通安全會報技術服務中心整理 |
| 1. 新建MRTG.bat檔 |

#### 開啟C:\inetpub\wwwroot\mrtg目錄中的網頁即可觀察視覺化的流量，詳見圖10。

|  |
| --- |
|  |
| 行政院國家資通安全會報技術服務中心整理 |
| 1. Windows MRTG視覺化的流量 |